ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
СОВЕТ МОЛОДЫХ УЧЕНЫХ
Евразийский национальный университет им.Л.Н.Гумилева

Студенттер мен жас ғалымдардың «ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2014» атты IX халықаралық ғылыми конференциясы

IX Международная научная конференция студентов и молодых ученых «НАУКА И ОБРАЗОВАНИЕ - 2014»

The IX International Scientific Conference for students and young scholars «SCIENCE AND EDUCATION-2014»

2014 жыл 11 сәуір
11 апреля 2014 года
April 11, 2014

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2014» атты IX Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ IX Международной научной конференции студентов и молодых ученых «Наука и образование - 2014»

PROCEEDINGS of the IX International Scientific Conference for students and young scholars «Science and education - 2014»

2014 жыл 11 сәуір

Астана

УДК 001(063)
ББК 72
Ғ 96

Ғ 96

«Ғылым және білім – 2014» атты студенттер мен жас ғалымдардың IX Халықаралық ғылыми конференциясы = IX Международная научная конференция студентов и молодых ученых «Наука и образование - 2014» = The IX International Scientific Conference for students and young scholars «Science and education - 2014». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2014. – 5831 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-610-4

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(063)
ББК 72

ISBN 978-9965-31-610-4

UDC004.056.55:004.773

REVIEW OF CRYPTOGRAPHIC ALGORITHM FOR INSTANT MESSENGER

Saukhanov Sultangazy
Faculty of Information Technology, Computer Science
Astana, Kazakhstan
saukhanov@gmail.com

Abstract: This article addresses problem of instant messaging (IM) security. Some part of data transferred across instant messenger is confidential and illegal access to it can result in significant costs to users. This paper will introduce suitable security approaches as a solution to security issues of IM.

Keywords: IM, instant messenger, cryptography, algorithm, real-time application

1. Introduction

Communication tool is an essential part of our life. Today there are several ways for communication, such as letters, telephone, email, and instant messaging. At the present time, instant messengers are very popular form of communication, because it is real-time application(RTA). IM applications have become available for PCs and mobile devices. Users communicate with each other by sending messages or transferring files via the Internet, or through local area network, if users locate within corporate network.

IM technology has become widely used in the corporate world. It is used to exchange information, in some cases, confidential data which had to be protected against cyber threats. Securing transaction between IM clients is vital to any organization that concerns about information confidentiality. According to Radicati Group Inc, it was expected growth of IM client up to 600 million in 2010. And every year number of IM users increases dramatically. Gartner states that 70% of employees use IM while at work. With the growth of popularity there is growth of security incidents. According to FaceTime Communication, IM threats increased more than twenty-fold from 2004 to 2005 [3].

Cyber criminals daily discover new ways of eavesdropping online conversations, intercepting transferred files in order to get profit.

There are several security vulnerabilities in IM applications. (Chavan, Aug 2003) According to results of survey made by CNet News among different IM providers, the in most IM applications is lack of message and file encryption. Confidential information transmitted through the IM application can be caught by intruders [1].

To solve the security issues have been stated above the developer requires cryptography algorithm which is suitable for RTAs.

The article is organized as follows: in section 2 we present AES, in section 3 we present RSA, in section 4 we present cryptographic algorithm for RTA, in section 5 we present RSA, in section 6 we give justification of chosen cryptography algorithm for RTA, in section 7we present conclusion of the research.

2. AES

AES (Advanced Encryption Standard) is the encryption standard of USA. It was accepted in 2000. Initiative in the development of AES owns NIST, in response to the growing feasibility of attacks against Data Encryption Standard (DES). AES specifies Rijndael algorithm. This algorithm is a symmetric block cipher that implemented on data block of 128-bit and uses a key length of 128, 192, and 256-bits. The algorithm can also be used with other lengths of data blocks and keys, but this option was not included was not included in the standard. US government stated that to break encryption with 128-bit sized key, it will take 149 trillion years [10].

AES is a fast algorithm; its implementation on simple processors is easy. Algorithm consists of strong mathematical foundations, such as substitution, transposition, exclusive OR (XOR), and addition operations. AES uses repeat cycles. For 128 bits key it uses 10 repeat cycles. Therefourstepineachcycle:

Bytesubstitution Each byte of 128-bit block is interchanged according to the substitution table in a substitution box.

Shiftrow This is transposition step for 128-bit block. Row *n* is changed its position left circular (n-1) bytes.

Mixcolumn This step involves both previous steps, row is shifted left and bits are XOR-ed with themselves.

Addsubkey To result of cycle the portion of unique key is XOR-ed.

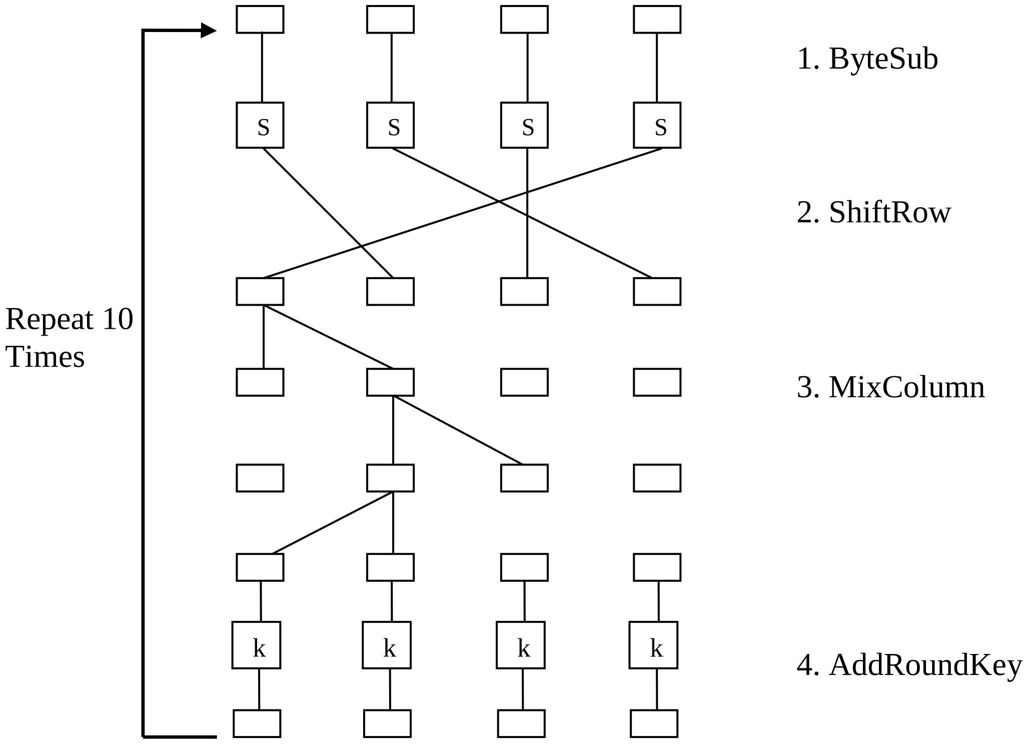

Figure 1. AES encryption process steps

3. RSA

RSA (Rivest-Shamir-Adleman) is the most commonly used public-key cryptographic algorithm. It was named after its inventors' name – Ron Rivest, Adi Shamir, Leonard Adleman. Among all public –key algorithms RSA is the most easiest to understand and implement. The security level of RSA is depends on the difficulty of factoring large numbers. The public and private keys are represented as a function of two large prime numbers. Numbers could consist in of 100 to 200 digits or even larger. (Schneier, 1996) To provide good security level the key size should be greater than 1024 bits. Key with 2048 bits size should give security for decades [10].

To generate private and public keys, it has to be chosen large prime numbers *p* and *q*, to provide maximum security level let them be equal length. Next step is to compute product of those prime numbers:

$n = p * q$

Encryption key, *e*, has to chosen randomly, such that *e* and $(p-1)(q-1)$ are relatively prime. To compute decryption key, *d*, the extended Euclidean algorithm has to be used. *d* has to be such that

$ed \equiv 1\, mod\, (p-1)(q-1)$

Itmeans

$d = e^{-1}\, mod\, ((p-1)(q-1))$

e and *n* are the public keys, and *d* is private key.

To encrypt the message *m*, *m* has to be divided into m_i blocks, such that$0 \leq e_i \leq n-1$. Theformulaofencryptingisfollowing

$c_i = m_i{}^e\, mod\, n$

To decrypt the encrypted message, the following computation has to be accomplished

$$m_i = c_i{}^d modn$$

RSA is currently the most secure public key algorithm, because of difficulties to factorize large numbers. However, speed of RSA processes is very slow, because computation of encryption/decryption processes include product of very large numbers (100 to 200 digit numbers). Therefore, RSA is mostly used by government, where resources are enough, to compute operations on such big numbers.

4. Blowfish

Blowfish is an algorithm designed by Bruce Schneier, intended for implementation on large microprocessors. According to the inventor, this algorithm is optimized for application where key does not change frequently. Blowfish is faster than DES when implemented on 32-bit microprocessors with large data caches, such as the Pentium. Blowfish has gained a fair amount of acceptance in a number of applications. There are no attacks known against Blowfish algorithm [10].

Blowfish is 64-bit block algorithm which consists of two parts: key expansion and data encryption. In the first part, key expansion converts key with size up to 448-bits into several subkey arrays. The total size of subkey arrays is 4168 bytes. The encryption part includes repeat cycles where simple function has to be performed. Cycles repeated 16 times. Each cycle consists of two processes. They are key dependent permutation, and a key- and data-dependent substitution. There are used addition and XOR function on 32-bit words. There is another additional operation for each round which is four indexed array data lookup. The subkeys have to be large numbers, and the keys must be computed before encryption and decryption processes. The Figure 2 represents the diagram of Blowfish's encryption/decryption processes. The Figure 3 represents F function which is used in each round.

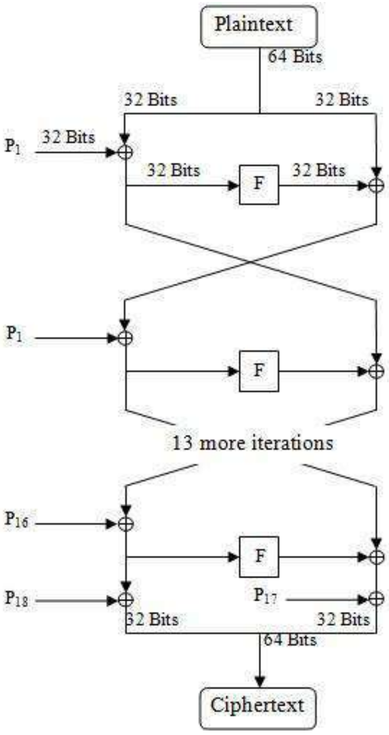

Figure 1– Blowfish[9].

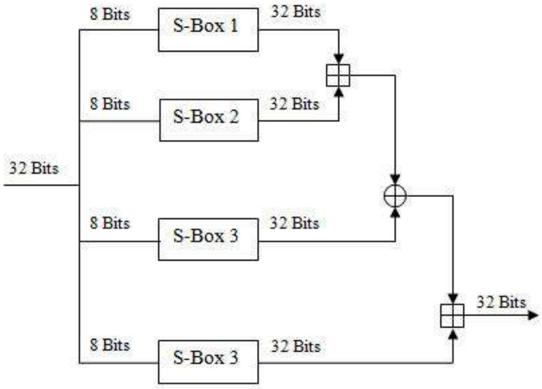

Figure 2 - Function F

5. Cryptographic algorithm for RTA

In 2008 Omari, A., et al, proposed new cryptographic algorithm which is provide fast encryption and decryption of data and higher level of security. Authors claim that the algorithm has minimum message delay, less than 400 milliseconds. One of the major factors in designing this algorithm is the time needed for encryption/decryption, where symmetric and asymmetric algorithm takes longer time. Another factor is the security level, it should be high enough so that attackers could not get the encryption/decryption key easily [6].

In this algorithm the key is very important to provide higher level of security. The key is 1024-bit long. The key is randomly chosen, to make it harder to intercept by attackers. Comparison made by authors between AES-Rijndael and proposed algorithm shows that encryption process of proposed algorithm is 15 times faster AES encryption, and decryption process is 6 times faster than AES decryption. Also this algorithm is resistant against brute force attack, because the key is mixed and shuffled strongly inside the XOR-ed data. Steps of proposed algorithm are described below.

First of all, the connection is initiated between participants by sending an initial packet. Initial packet is based on the operations performed at the sender side. The operations are performed according to a shared mathematical formula. The operations are the follows: the construction of an initial random generator table which is based on a mathematical formula; the mathematical formula is shared and known previously, by using the formula the same table values are initialized at the both sender and receiver sides. As shown in the Figure 4, the table size is *16x16* columns and rows. The range of entry values is between 0-9.

Steps at the sender side:

1. 1024 – bits size key is randomly chosen;
2. Data is encrypted by XOR-ing with the key
3. The key is inserted in the XOR-ed data by using indexes generated earlier from the shifted table;
4. Thepackedissent.

Steps at the receiver side:

1. The key is extracted out of the packet by using the shifted generated table;
2. Data is decrypted by XOR-ing with the key [6].

1	8	1	0	5	6	3	6	5	2	1	8	1	0	5	6
8	8	0	4	0	8	8	0	4	2	8	8	0	4	0	8
1	0	7	2	5	6	5	2	7	2	1	0	7	2	5	6
0	4	2	4	9	9	4	2	4	2	0	4	2	4	0	0
5	0	5	0	5	0	5	0	5	2	5	0	5	0	5	0
6	8	6	0	0	6	8	6	0	2	6	8	6	0	0	6
3	8	5	4	5	8	3	0	9	2	3	8	5	4	5	8
6	0	2	2	0	6	0	2	2	2	6	0	2	2	0	6
5	4	7	4	5	0	9	2	9	2	5	4	7	4	5	0
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
1	8	1	0	5	6	3	6	5	2	1	8	1	0	5	6
8	8	0	4	0	8	8	0	4	2	8	8	0	4	0	8
1	0	7	2	5	6	5	2	7	2	1	0	7	2	5	6
0	4	2	4	0	0	4	2	4	2	0	4	2	4	0	0
5	0	5	0	5	0	5	0	5	2	5	0	5	0	5	0
6	8	6	0	0	6	8	6	0	2	6	8	6	0	0	6

Figure 4.An Initial Random Generator Table

Following is a table of comparisons of cryptographic algorithms summarized from the above introductions:

Algorithm	**Security level**	**Speed**	**Key Size**
RSA	Very Secure	Very slow	Recommended to set 1024-bits or more
AES	Secure	Slow	128, 192, 256-bit
Blowfish	Not	Fast	32 – 448-bit
New cryptography algorithm for RTA	Very secure	Very fast	1024-bit

Table 1. Comparison between encryption algorithms

6. Justification of chosen cryptography algorithm

Based on the research carried out, proposed new encryption algorithm is suitable for Instant Messenger. The reason of selecting new encryption algorithm instead RSA, Blowfish and AES is that originally it was designed as encryption algorithm for Real-Time Applications. Omari et al, claimed that new proposed encryption algorithm has a minimum message delay, which is vital for Real-Time Applications, and better security level compared with other well-known algorithm, such as AES. The result of comparison, stated in the table below, showed that new algorithm's encryption and decryption processes are 15 and 9 times faster than AES's encryption and decryption processes, respectively. That is advantage of new algorithm over AES and RSA algorithms.

Security Algorithm	AES-RSA	New proposed algorithm
Encryption (ms)	10.884	0.71575
Decryption (ms)	10.718	1.958125

Table 2. Comparison between AES-Rjindael and the New algorithm

Advantage of new proposed encryption algorithm over Blowfish is that new algorithm provides higher level of security which is based on size of key. With 1024-bits key size new algorithm's encryption and decryption processes are significantly fast, whereas Blowfish is fast by 56-bits key size. If encryption/decryption processes will be performed with 1024-bits size, the speed will be very slow, because of 16 times repeat cycles.

The key advantage of new proposed algorithm is its resistance against brute force attacks, because the key is mixed with the XOR-ed encrypted data. Therefore, it is very difficult to find the key by guessing it[6].

7. Conclusion

Research in this article has been made in the Instant Messaging technology area. We have identified security problems of the existing popular IM applications and have proposed solution for it. We have chosen suitable cryptography algorithm to encrypt messages.

The proposed system was successfully developed within the given time frame. All the main objectives have been achieved; therefore the system works in proper condition. This is the one of the biggest, individually completed project by developer.

References

1. Chavan, S., 2003, *Understanding Instant Messaging (IM) and its security risks*, SANS Institute

2. Hindocha, N., 2003, *Instant Insecurity: Security issues of Instant Messaging*, 2003, Symantec

3. Korzeniowski, P., 2004, *Instant Messaging Opens New Security Holes[online]*, Available from http://www.technewsworld.com/story/33271.html, Accessed on 13th October 2013

4. McOullagh, D, 2008, *How safe is instant messaging? A security and privacy survey[online]*, Available on http://news.cnet.com/8301-13578_3-9962106-38.html, Accessed on 20th October 2013

5. Ollman, G., *Instant Messenger Security: Securing Against the Threat of Instant Messengers[online]*, Available on http://www.windowsecurity.com/whitepapers/Instant-Messenger-Security.html, Accessed on 22nd of October 2013

6. Omari, A. H., Al-Kasasbeh, B. M., Al-Qutaish, R. E., and Muhairat, M. I., *A New Cryptographic Algorithm for the Real Time Applications*, 2008

7. Piccard. P., Sachs, M., Baskin. B., 2006, *Securing IM and P2P Applications for Enterprise*, United States of America , Syngress Publishing

8. Schneier, B., 1996, *Applied Cryptography*, Canada, John Wiley and Sons, Inc

9. Stallings, W., 2006, *Cryptography and Network Security*, United States of America, Pearson Education, Inc

10. Tech Corner, 2000, "*Cryptographic algorithms*" *[online]*, Available from http://www.dei.isep.ipp.pt/~andre/normas/algorithms.htm, Accessed on 13th February 2014